ISSN 1561-5359. Штучний інтелект, 2020, № 2

УДК 004.8; 004.7

О.М. Юнак[1,2]***, Б.М. Стрихалюк***[1]***, О.П. Юнак***[2]
[1]Національний університет «Львівська політехніка», Україна
вул. Степана Бандери, 12, м. Львів, 79000
[2]Відокремлений структурний підрозділ «Коледж телекомунікацій та комп'ютерних технологій» Національного університету «Львівська політехніка», Україна
вул. Володимира Великого, 12, м. Львів, 79000

ШИФРУВАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ МАТРИЦЬ ПЕРЕТВОРЕНЬ ДЛЯ ЗАХИСТУ ВІД ДЕШИФРУВАННЯ НЕЙРОННИМИ АЛГОРИТМАМИ

O.M. Yunak[1,2]***, B.M. Strykhaliuk***[1]***, O.P. Yunak***[2]
[1]Lviv Polytechnic National University, Ukraine
12, Stepana Bandery St., Lviv, 79000
[2]Separated structural unit «College of telecommunications and computer technologies» of National University «Lviv Polytechnic», Ukraine
12, Volodymyra Velykoho St., Lviv, 79000

ENCRYPTION OF GRAPHIC INFORMATION BY MEANS OF TRANSFORMATION MATRIXES FOR PROTECTION AGAINST DECODING BY NEURAL ALGORITHMS

У статті розглядається алгоритм шифрування графічної інформації (зображень) за допомогою матриць перетворень. Розглянуто дії, які можна зробити із зображенням. Наведені алгоритми формування матриць, які сформовані за допомогою випадкових процесів. Показані приклади матриць та результати шифрування. Проведені розрахунки аналізу комбінацій та висновки по них. Продемонстровані можливості та переваги даного алгоритму шифрування зображень. Запропонований алгоритм дозволить передавати шифровану інформацію відкритими каналами зв'язку. В алгоритмі використано всі можливі дії, котрі можна зробити із зображенням: змінено розмір зображення, додано надлишкові елементи до зображення, змінено розташування пікселів, змінено яскравість пікселів зображення, інвертовано пікселі зображення, змінено кольори пікселів зображень. Рандомізований підхід формування матриць унеможливить використання нейронних систем. Алгоритм досить простий в реалізації написання коду шифрування. Дешифрування зображення без ключа стає неможливим, так як кількість можливих комбінацій є надзвичайно великою. Алгоритм можна використовувати у військовій галузі, у розвідці, у сферах захисту інформації. Шифрування не потребує значних обчислювальних ресурсів та ресурсів оперативної пам'яті. Даний алгоритм може бути реалізований у WEB-технологіях та в мобільних додатках, в ньому відсутні рекурсивні функції та цикл у циклі. Алгоритм ховає розмір зображення, це, в свою чергу, додає додатковий захист. Надлишкові елементи не дозволять нейронним мережам співставляти пікселі. Зміна кольорів, зміна яскравості, інверсія за допомогою випадкових процесів не дозволить нейронним мережам підібрати функцію розшифрування. У статті розглядається алгоритм шифрування зображень, який дозволить сформувати ключ. Ключ являтиме собою набір двовимірних масивів, сформованих рандомізованим способом. Рандомізований підхід формування матриць унеможливить використання нейронних систем. У алгоритмі використано всі можливі дії, котрі можна зробити із зображенням, а саме: змінено розмір зображення, додано надлишкові елементи до зображення, змінено розташування пікселів, змінено яскравість пікселів зображення, інвертовано пікселі зображення, змінено кольори пікселів зображень. Матриця зміни розташування пікселів дає нам (Nx · Ny)! комбінацій. Матриця зміни яскравості пікселів дає нам 8*(Nx · Ny)! комбінацій. Матриця інвертації пікселів дає нам 8*(Nx · Ny)! комбінацій. Матриця зміни кольору пікселів дає нам 6*(Nx · Ny)! комбінацій. Загальна кількість комбінацій N рівна: дешифрування зображення без ключа стає неможливим, так як кількість можливих комбінацій є надзвичайно великою. Алгоритм досить простий в реалізації написання коду шифрування. Алгоритм можна використовувати у військовій галузі, у розвідці, у сферах захисту інформації. Перевагою такого алгоритму є те, що зашифроване зображення можна передавати відкритими каналами.

Ключові слова: шифрування, дешифрування, графічна інформація, матриці перетворення, захист, нейронні алгоритми, випадкові процеси, зображення, RGB, ключ шифрування

The article deals with the algorithm of encrypting graphic information (images) using transformation matrixes. It presents the actions that can be done with the image. The article also gives algorithms for forming matrixes that are created with the use of random processes. Examples of matrixes and encryption results are shown. Calculations of the analysis of combinations and conclusions to them are carried out. The article shows the possibilities and advantages of this image encryption algorithm. The proposed algorithm will allow to transmit encrypted information through open communication channels. The algorithm uses all possible actions that can be done with the image, namely: image resizing, adding redundant elements to the image, changing the location of the pixels, changing the brightness of the image pixels, inverting the image pixels, changing the colours of the images pixels. A randomized approach to matrix formation will make it impossible to use neural systems. The algorithm of the implementation of writing encryption code is rather simple. It is not possible to decrypt the image without a key as the number of possible combinations is extremely large. This algorithm can be used in the military, intelligence, information security. Encryption does not require significant computing or RAM resources. This algorithm can be implemented in WEB-technology and in mobile applications, it has no recursive functions and loop in loop. The algorithm hides the image size, which in turn adds extra protection. Redundant elements will not allow neural networks to compare pixels. Changing colors, changing brightness, inversion by random processes will not allow neural networks to find the decryption function. The article considers an image encryption algorithm that will give a possibility to generate a key. The key will be a set of two-dimensional arrays formed in a randomized manner. A randomized approach to matrix formation will make it impossible to use neural systems. The algorithm uses all possible actions that can be done with the image, namely: (1) Image resizing. (2) Adding redundant elements to the image. (3) Changing the location of the pixels. (4) Changing the brightness of the image pixels. (5) Inverting the image pixels. (6) Changing the colours of the images pixels. The pixel positioning matrix gives us (Nx • Ny)! combinations. The pixel brightness change matrix gives us 8 * (Nx • Ny)! combinations. The pixel inversion matrix gives us 8 * (Nx • Ny)! combinations. The pixel colour change matrix gives us 6 * (Nx • Ny)! Combinations. The total number of combinations N is equal to: It is not possible to decrypt the image without a key as the number of possible combinations is extremely large. The algorithm of the implementation of writing encryption code is rather simple. This algorithm can be used in the military, intelligence, information security. The advantage of this algorithm is the fact that the encrypted image can be transmitted through open channels.

Keywords: encryption, decryption, graphic information, matrix transformation, security, neural algorithms, random processes, image, RGB, encryption key

Вступ

Постановка проблеми

Сучасні системи передачі графічної інформації потребують надійного захисту даних, на даний момент немає 100% гарантій, що зловмисники не зможуть отримати доступ до системи. Надійне шифрування унеможливить зловживання інформацією. Сучасні нейронні алгоритми навчені за короткий час розшифрувати інформацію, це зумовлено тим, що більшість систем шифрування використовують афінні перетвореннях, функції (ітераційні функції) [1, 3, 4], системи функцій. Розробка алгоритму шифрування, який буде використовувати ключ у вигляді набору матриць перетворень, сформованих за допомогою випадкових процесів, унеможливить дешифрування нейронними мережами.

Аналіз останніх досліджень і публікацій

Деякими науковцями започатковано розв’язання даної проблеми. Такі науковці, як Ю.М. Рашкевич, А.М. Ковальчук, Д.Д. Пелешко [2, 3], Н.О. Кустра, Н.Д. Лотошинська, В.Г. Красиленко, С.К. Грабовляк [4], К.С. Попадинець, І.А. Хижняк та інші присвятили різним аспектам шифрування та дешифрування зображень багато уваги. На дослідження науковців спираються автори цієї статті.

Мета дослідження

Розробка алгоритму шифрування й дешифрування зображення з використанням матриць перетворень, які формуються випадковими процесами для захисту від дешифрування нейронними алгоритмами.

Виклад основного матеріалу

Дії, які можна зробити із зображенням: (1) змінити розмір зображення; (2) додати надлишкові пікселі (інші зображення); (3) змінити розташування пікселів; (4) змінити яскравість пікселів зображення; (5) інвертувати пікселі; (6) змінити кольори пікселів зображень.

Кожна з цих дій буде кроком нашого алгоритму шифрування.

Змінити розмір зображення

Візьмемо базове зображення з розмірами N_{x0} x N_{y0} і розмістимо його на білому фоні з розмірами N_x x N_y з умовою, що $N_{x0} < N_x/2$ і $N_{y0} < N_y/2$ та з умовою, що на граничних лінія y_0 та x_0 буде хоча б по одному пікселю небілого кольору (рис. 1).

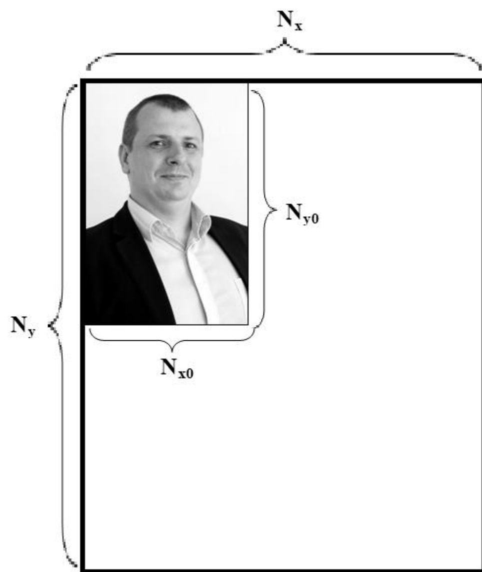


Рис. 1. Зміна розміру зображення

Додаємо інші надлишкові зображення

Для цього повинна бути сформована база випадкових зображень з розмірами M_x x M_y з умовою, що $M_x = N_x/2$ і $M_y = N_y/2$ та розташовуємо їх так, щоб вони торкалися інших протилежних кутів (рис. 2).



Рис. 2. Надлишкові зображення

Змінюємо розташування пікселів

Створюємо двовимірну матрицю з розмірами [i, j], де $i = N_x – 1$, $j = N_y – 1$ та розташовуємо у випадковому порядку (без повторень) числа від 1 до $N_x \cdot N_y$. Тепер беремо по-порядку, зліва направо та згори до низу кожну точку нашого зображення (рис. 2) переносимо на нове місце, за наступним правилом $x_n = i' +1$, $y_n = j' +1$, де i′, j′ - це координати цифри, яка відповідає порядковому номеру пікселя n (рис. 3, рис. 4).

j *i*

5	10	200	287	895
36	100	148	6	637
95	3	235	179	630
698	98	1	12	638
105	336	543	286	88

Рис. 3. Матриця переміщень пікселів

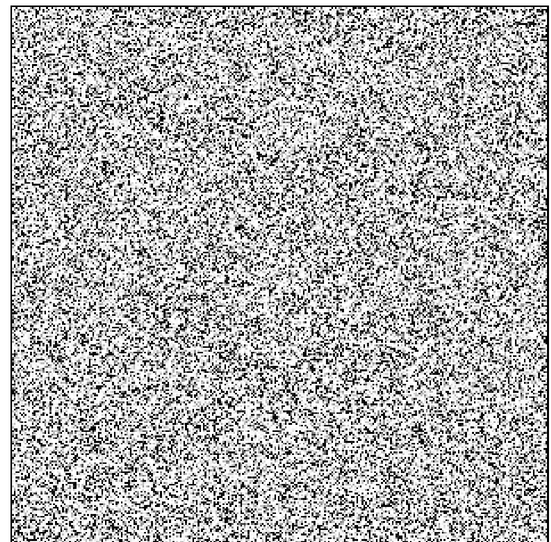


Рис. 4. Результати переміщення пікселів

Зміна яскравості пікселів

Сформуємо двовимірну матрицю з розмірами [i, j], де $i = N_x – 1$, $j = N_y – 1$ та розташовуємо у випадковому порядку (без повторень) числа від 0 до 7 (рис. 5), де: 0 – не змінювати яскравість; 1 – зменшити наполовину яскравість червоного кольору (R) колірної моделі RGB; 2 – зменшити наполовину яскравість зеленого кольору (G); 3 – зменшити наполовину яскравість синього кольору (B); 4 – зменшити наполовину яскравість червоного й зеленого кольорів; 5 – зменшити наполовину яскра-

вість червоного й синього кольорів; 6 – зменшити наполовину яскравість зеленого й синього кольорів; 7 – зменшити наполовину яскравість всіх кольорів.

7	1	0	7	4
6	2	3	3	5
0	3	4	4	5
3	0	1	6	2
5	7	2	6	0

Рис. 5. Матриця змін яскравості

Проведемо інвертацію пікселів

Сформуємо двовимірну матрицю з розмірами [i, j], де $i = N_x - 1$, $j = N_y - 1$ та розташовуємо у випадковому порядку (без повторень) числа від 0 до 7 (рис. 8), де: 0 – не змінювати піксель; 1 – здійснити інвертацію червоного кольору пікселя (R) колірної моделі RGB; 2 – здійснити інвертацію зеленого кольору (G); 3 – здійснити інвертацію синього кольору (B); 4 – здійснити інвертацію червоного й зеленого кольорів; 5 – здійснити інвертацію червоного й синього кольорів; 6 – здійснити інвертацію зеленого й синього кольорів; 7 – здійснити інвертацію всіх кольорів.

0	1	3	5	6
1	7	6	3	5
6	3	0	5	5
4	0	4	7	2
5	7	1	6	6

Рис. 6. Матриця змін інвертацій

Змінюємо кольори пікселів

Аналогічно до попередніх пунктів, формуємо двовимірну матрицю з розмірами [i, j], де $i = N_x - 1$, $j = N_y - 1$ та розташовуємо у випадковому порядку (без повторень) числа від 0 до 5 (рис. 7), де: 0 – без змін; 1 – червоний змінюємо із синім значенням кольорів кольорової моделі RGB; 2 – червоний змінюємо із зеленим значенням кольорів; 3 – синій змінюємо із зеленим значенням кольорів кольорової моделі RGB; 4 – червоний ставимо на місце синього, синій - на місце зеленого, а зелений – на місце червоного; 5 – червоний ставимо на місце зеленого, зелений – на місце синього, а синій – на місце червоного.

5	3	1	5	4
0	2	4	3	5
4	3	0	5	5
2	1	4	4	2
0	2	1	0	1

Рис. 7. Матриця змін кольорів

Результат виконання шифрувань матрицями перетворень, сформованих за допомогою випадкових процесів:

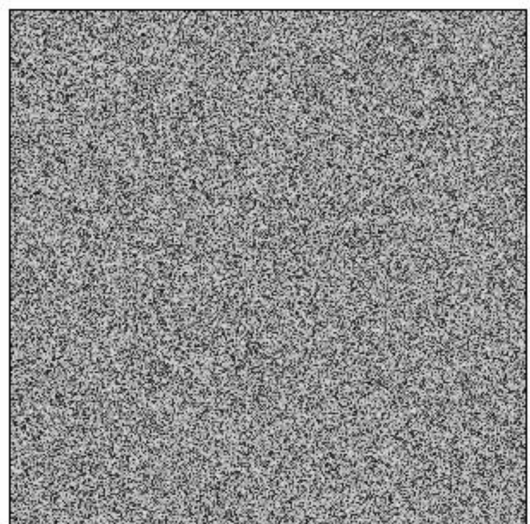


Рис. 8. Результат шифрування

Аналіз можливих комбінацій

Так як всі матриці формувалися випадковим чином і мають ¾ надлишковос-

ті, нейронна мережа змушена буде проходити по всіх можливих комбінаціях:

Матриця зміни розташування пікселів дає нам $(N_x \cdot N_y)!$ комбінацій.

Матриця зміни яскравості пікселів дає нам $8*(N_x \cdot N_y)!$ комбінацій.

Матриця інвертації пікселів дає нам $8*(N_x \cdot N_y)!$ комбінацій.

Матриця зміни кольору пікселів дає нам $6*(N_x \cdot N_y)!$ комбінацій.

Загальна кількість комбінацій N рівна:

$$N = 384 \cdot \left(\left(N_x \cdot N_y\right)!\right)^4 \quad (1)$$

де $N_x \cdot N_y$ – кількість пікселів зображення з надлишковістю з умовою, що $N_{x0} < N_x/2$ і $N_{y0} < N_y/2$. Таким чином, кількість комбінацій N відповідає вимогам:

$$N \approx 384 \cdot \left(4! \cdot \left(N_{x0} \cdot N_{y0}\right)!\right)^4 = 128065536 \cdot \left(\left(N_{x0} \cdot N_{y0}\right)!\right)^4 \quad (2)$$

Розрахуємо кількість комбінацій, якщо кількість пікселів зображення $N_{x0} \cdot N_{y0}$ буде складати 1, 10, 100, 1000 пікселів. Результати зведемо в таблицю 1.

Таблиця 1. Кількість комбінацій

$N_{x0} \cdot N_{y0}$	N
1	128065536
10	$4{,}6 \cdot 10^{14}$
100	$1{,}19 \cdot 10^{166}$
1000	$5.1 \cdot 10^{2576}$

Дешифрування зображення

Спробуємо відтворити зображення, виконавши протилежні дії, відповідно до матриць, які були сформовані (рис. 9).



Рис. 9. Результат дешифрування

Висновки

Даний алгоритм досить простий в реалізації написання коду шифрування. Він дає можливість створювати ключ шифрування, без нього неможливо розшифрувати зображення. Алгоритм ховає розмір зображення, це, в свою чергу, додає додатковий захист. Надлишкові елементи не дозволять нейронним мережам співставляти пікселі. Зміна кольорів, зміна яскравості, інверсія за допомогою випадкових процесів не дозволить нейронним мережам підібрати функцію розшифрування. Нейронні мережі не можуть визначити функцію шифрування, так як матриці формуються випадковим чином. Щоб розшифрувати зображення з 1000 пікселів, доведеться перебрати більше, ніж $5.1 \cdot 10^{2576}$ комбінацій, що, на даний момент, не є технічно можливим рішенням. Алгоритм ховає розмір зображення, це, в свою чергу, додає додатковий захист. Надлишкові елементи не дозволять нейронним мережам співставляти пікселі. Зміна кольорів, зміна яскравості, інверсія за допомогою випадкових процесів не дозволить нейронним мережам підібрати функцію розшифрування. Отже, даний алгоритм можна використовувати у військовій галузі, у розвідці, у сферах захисту інформації. Перевагою такого алгоритму є те, що зашифроване зображення можна передавати відкритими каналами.

Література

1. В. Ємець *Сучасна криптографія: Основні поняття /* В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.: іл.
2. Рашкевич, Ю.М., Пелешко, Д.Д., Ковальчук, А.М., Пелешко, М.З. (2008) Модифікація алгоритму RSA для деяких класів зображень. *Технічні вісті* 1(27), 2(28). С. 59 – 62.
3. Y. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak. (2009) Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. *Proceedings of the X-th International Conference CADSM*. 24-28 February 2009, Lviv-Polyana, Ukraine, Pp. 469-473.
4. Красиленко, В.Г., Грабовляк, С.К. (2012) Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень. *Системи обробки інформації.* № 3(101). – С. 53-61 Вінниця.

5. Красиленко, В.Г., Огородник, К., Флавицька, Ю. (2010) Моделювання матричних афінних алгоритмів для шифрування кольорових зображень, *Комп'ютерні технології: наука і освіта*: тези доповідей V Всеукр. наук.-пр. конф. – К., 2010. – С. 120-124.
6. Красиленко, В.Г., Нікольський, О.І., Лазарєв, О.О. (2008) Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях. *Наука і навчальний процес: науково-методичний збірник науково-практичної конференції*. – Вінниця, 2008. – С. 107-109.
7. Красиленко, В.Г., Грабовляк, С.К., (2011) Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи. *Системи обробки інформації*: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 7 (97). – С. 60-63.
8. Красиленко, В.Г., Свіренюк, С.А. (2006) Розробка методу криптографічного захисту інформації текстографічного типу. *Наука і навчальний процес: науково-методичний збірник науково-практичної конференції*. – Вінниця, 2006. – С. 73-74.
9. Красиленко В.Г., Грабовляк, С.К. (2012) Оцінювання стійкості та часу зламування у матрично-перестановочних алгоритмах криптоперетворень. *Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна"*. – Вінниця, 2012. – С. 173-174.
10. Красиленко, В.Г., Грабовляк, С.К. (2012) Моделювання матричного афінно-перестановочного алгоритму для криптоперетворень зображень. *Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна"*. – Вінниця, 2012. – С. 171-172.

References

1. V. Jemecʹ Sučasna kryptohrafija: Osnovni ponjattja / V. Jemecʹ, A. Melʹnyk, R. Popovyč. – Lʹviv: BaK, 2003. – 144 s.: il.
2. Raškevyč, Ju.M., Peleško, D.D., Kovalʹčuk, A.M., Peleško, M.Z. (2008) Modyfikacija alhorytmu RSA dlja dejakych klasiv zobraženʹ. Techničnі visti 1(27), 2(28). S. 59 – 62.
3. Y. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak. (2009) Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM. 24-28 February 2009, Lviv-Polyana, Ukraine, Pp. 469-473.
4. Krasylenko, V.H., Hrabovljak, S.K. (2012) Matryčni afinno-perestanovočni alhorytmy dlja šyfruvannja ta dešyfruvannja zobraženʹ. Systemy obrobky informacії. # 3(101). – S. 53-61 Vinnycja.
5. Krasylenko, V.H., Ohorodnyk, K., Flavycʹka, Ju. (2010) Modeljuvannja matryčnyx afinnyx alhorytmiv dlja šyfruvannja kolʹorovyx zobraženʹ, Kompjuterni texnolohiji: nauka i osvita: tezy dopovidej V Vseukr. nauk.-pr. konf. – K., 2010. – S. 120-124.
6. Krasylenko, V.H., Nikolʹsʹkyj, O.I., Lazarjev, O.O. (2008) Modeljuvannja modyfikovanoho alhorytmu stvorennja 2-D ključa v kryptohrafičnyx zastosuvannjax. Nauka i navčalʹnyj proces: naukovo-metodyčnyj zbirnyk naukovo-praktyčnoji konferenciji. – Vinnycja, 2008. – S. 107-109.
7. Krasylenko, V.H., Hrabovljak, S.K., (2011) Matryčni afinni šyfry dlja stvorennja cyfrovyx slipyx pidpysiv na tekstohrafični dokumenty. Systemy obrobky informaciji: zb. nauk. pr. – X.: XUPS, 2011. – Vyp. 7 (97). – S. 60-63.
8. Krasylenko, V.H., Svirenjuk, S.A. (2006) Rozrobka metodu kryptohrafičnoho zaxystu informaciji tekstohrafičnoho typu. Nauka i navčalʹnyj proces: naukovo-metodyčnyj zbirnyk naukovo-praktyčnoji konferenciji. – Vinnycja, 2006. – S. 73-74.
9. Krasylenko V.H., Hrabovljak, S.K. (2012) Ocinjuvannja stijkosti ta času zlamuvannja u matryčno-perestanovočnyx alhorytmax kryptoperetvorenʹ. Nauka i navčalʹnyj proces: naukovo-metodyčnyj zbirnyk materialiv naukovo-praktyčnoji konferenciji VSEI Universytetu "Ukrajina". – Vinnycja, 2012. – S. 173-174.
10. Krasylenko, V.H., Hrabovljak, S.K. (2012) Modeljuvannja matryčnoho afinno-perestanovočnoho alhorytmu dlja kryptoperetvorenʹ zobraženʹ. Nauka i navčalʹnyj proces: naukovo-metodyčnyj zbirnyk materialiv naukovo-praktyčnoji konferenciji VSEI Universytetu "Ukrajina". – Vinnycja, 2012. – S. 171-172.

Надійшла до редакції 03.02.2020

